

### REMARKS

The claims have been amended to more clearly define the invention as disclosed in the written description. In particular, the claims have been amended for clarity.

Applicant believes that the above changes answer the Examiner's 35 U.S.C. 112, paragraph 2, rejection of the claims, and respectfully requests withdrawal thereof.

The Examiner has rejected claims 1-14 and 16 under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter, in that the claims are rejected as not being tangible as they may be implemented solely in software.

Applicant submits that the Examiner is mistaken. In particular, claim 1 includes the limitation "exchanging authentication data between said first unit and said second unit, said authentication data being retrieved from an authorization list comprising a list identifier". Applicant submits that this limitation cannot be implemented solely in software. Further, the invention as claimed in both claims 12 and 16 is clearly an apparatus claim including a first unit and a second unit.

The Examiner has rejected claims 1-16 under 35 U.S.C. 102(b) as being anticipated by U.S. Patent 5,949,877 to Traw et al.

The Traw et al. patent discloses content protection for transmission systems, in which the device to be authorized is

compared to a revocation list, and if the device appears on the list, the device is not authorized.

Applicant submits that the Examiner is mistaken. In particular, to shows the differences between the subject matter of Traw et al. and the present invention more clearly, enclosed herewith are two Figures A and B, in which Figure A shows the use of a revocation list ("black-listing") as described in Traw et al., while Figure B shows the use of an authentication list ("white-listing") according to the claimed invention. It should be noted that these figures only show the essential steps for understanding the difference.

There are some major differences between the two systems:

(a) data stored in units:

(a1) In Traw et al., as shown in Figure A, every unit stores a certificate (cert) on its own public key (PK); and a revocation list (CRL) with version number (CRLV) on which the ID's of revoked devices reside. The length of this list is generally proportional to the total number of revoked devices (and could be several hundreds of kilobytes or more).

(a2) in the subject invention, as shown in Figure B, every unit stores a certificate (cert) on its own public key (PK); an authorization list (CAL) with version number (CALV) on which ID's of devices reside that are still authenticated. Typically, this list only contains the ID of the device itself (an possibly a few

more), but it is not dependent on the number of devices revoked so far, or the total number of devices; and a required authorization list version number (CALV) (against which the CALV on an CAL submitted by a prover is to be compared).

(b) checks performed:

(b1) In Traw et al. as shown in Figure A, every verifier checks that the (signature on the) certificate of the prover is okay; and the ID of the prover is not on the CRL.

(b2) In the subject invention as shown in Figure B, the (signature on the) certificate of the prover is okay; the ID of the prover is on the authorization list supplied by the prover; the (signature on the) supplied authorization list from the prover is okay; and the CALV on the authorization list from the prover is greater/equal to the CALV stored in the verifier (i.e., validity of the CAL is checked).

(c) revocation/authorization information updating after authentication checks:

(c1) In Traw et al. as shown in Figure A, the CRL needs to be downloaded from the other party if the CRLV of the other party is more recent.

(c2) In the subject invention as shown in Figure B, the CALV is simply updated if the CALV (in the CAL) of the other party is more recent. No further data exchange is needed.

Applicant submits that in the present invention (Figure B), the verifier has to do more work (e.g., check 2 signatures, etc.), but has the advantage of only having to store a short CALV instead of a potentially long CRL. Further, the updating is simpler in the subject invention, i.e., the use of an authentication list has many advantages over the use of a revocation list.

Another difference between the user of a revocation list and an authentication list is that the CRL must always be transmitted/stored/interpreted in its entirety (if only, e.g., the first half is stored and a device from the second half presents itself to a prover, it cannot be sure whether it is revoked or not). The CAL, on the other hand, can be cut into pieces: if there is a certain device, one can just cut out the part of the CAL that refers to this device and go to a verifier with the corresponding public key certificate and this small part of the white-listing (CAL) to show that this device is not revoked (at least not with the current CALV, which is the reason why the verifier needs to store the CALV itself, and cannot rely on the prover for that).

Hence, in practice, (employing the invention) the trusted third party (TTP) will cut the CAL into many small CAL's (maybe one for every device, or, for efficiency, one CAL for every, e.g., 10 devices, with 10 device ID's on such CAL), and sign them separately. This can never be done with CRL's as disclosed in Traw et al.

The question of the size of the "sub-CAL's is a separate optimization question (one could even imagine that in the beginning when there are few devices, there is only 1 sub-CAL, and after a while, it gets split more and more.

Still further, in the case of Traw et al., as regard the feature "validity of revocation list", it is implied that the revocation list is recent enough. In the case of the present invention, however, as regards the feature, in addition to this meaning of Traw et al., an additional check is made to make sure that it isn't some old proof.

Hence, Applicant submits that although there are similarities between Traw et al. and the subject invention, there are many important differences leading to certain advantages of each solution. Consequently, Applicant submits that it is neither anticipated nor obvious to simply replace the revocation list of Traw et al. by an authentication list.

First, there is no motivation for the skilled person to modify the solution known from Traw et al. The solution known from Traw et al. works, and there is no hint why the skilled person would change from this working solution.

Second, such a modification would not be as simple as it seems. Simply replacing the revocation list by an authentication list would not be sufficient to have a working solution, but additional/different steps, in particular, for checking the


validity and for updating (see the differences if Figures A and B), are required.

Third, even if such a replacement were made, the result would not be the solution as claimed in claims 1 and 12. At least step c) is still missing which is neither disclosed nor suggested by Traw et al.

In view of the above, Applicant believes that the subject invention, as claimed, is neither anticipated nor rendered obvious by the prior art, and as such, is patentable thereover.

Applicant believes that this application, containing claims 1-16, is now in condition for allowance and such action is respectfully requested.

Respectfully submitted,

by   
Edward W. Goodman, Reg. 28,613  
Attorney  
Tel.: 914-333-9611

CERTIFICATE OF MAILING

It is hereby certified that this correspondence is being deposited with the United States Postal Service as First-class mail in an envelope addressed to:

COMMISSIONER OF PATENTS AND TRADEMARKS  
P.O. BOX 1450  
ALEXANDRIA, VA 22313-1450

On October 06, 2005  
By Burnett James